VPN-etäyhteydet (Cisco AnyConnect)

Tämä ohje on vanhentunut

Cisco AnyConnect on poistettu käytöstä Metropoliassa. Ota käyttöön Palo Alto GlobalProtect VPN ohjeen mukaan.

- VPN-yhteys GlobalProtect-palvelun kautta
- VPN-yhteys GlobalProtect-palvelun kautta, PopJazz Konservatorio ja Helsingin Konservatorio

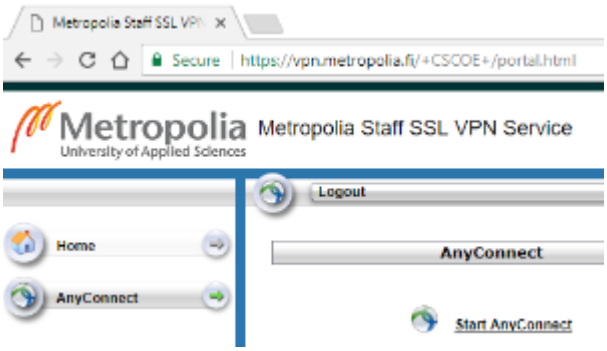
Kaikilla Metropolian käyttäjillä on käytettävissään VPN-etäyhteys. Etäyhteyttä tarvitaan, kun käytetään sisäisiä palveluita Metropolian toimipisteiden ulkopuolelta. Sisäisistä palveluista esimerkkejä ovat mm. talous- ja henkilöstöhallinnon palvelut, Koulutuskalenteri sekä opetusta tukevat projektipalvelimet, educloud ja laboratorioiden järjestelmät. VPN-etäyhteydellä saatava pääsy sisäverkkoon määräytyy käyttäjän roolin ja päätelaitteen perusteella.

VPN-apuohjelman asennus ja käyttö omissa tietokoneissa

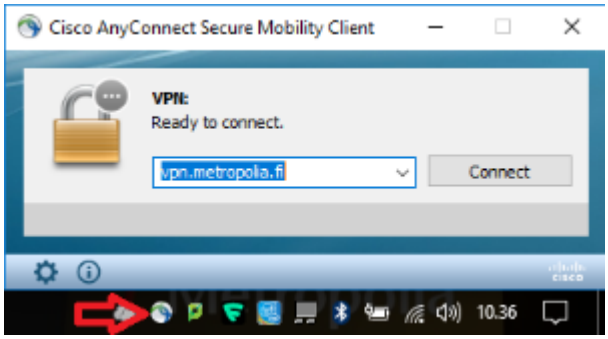
VPN-etäyhteyden käyttämiseen tarvitaan AnyConnect-apuohjelma. Se on esiasennettuna Metropolian ylläpitämiin tietokoneisiin. Tätä apuohjelmaa ei saa asentaa eikä päivittää Metropolian ylläpitämiin tietokoneisiin.

Omiin laitteisiin (Windows- ja Mac-tietokoneet) käyttäjä asentaa AnyConnect-apuohjelman itse.

1. Kirjaudu osoitteeseen https://vpn.metropolia.fi
2. Valitse vasemmalta AnyConnect.
3. Valitse Start AnyConnect.



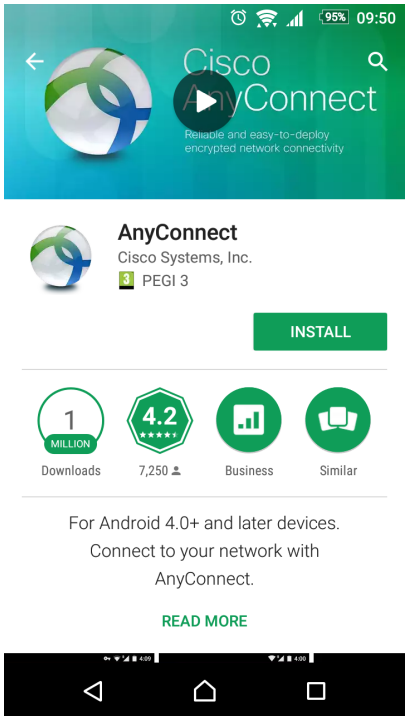
4. Kirjaudu osoitteeseen vpn.metropolia.fi tai osoitteeseen



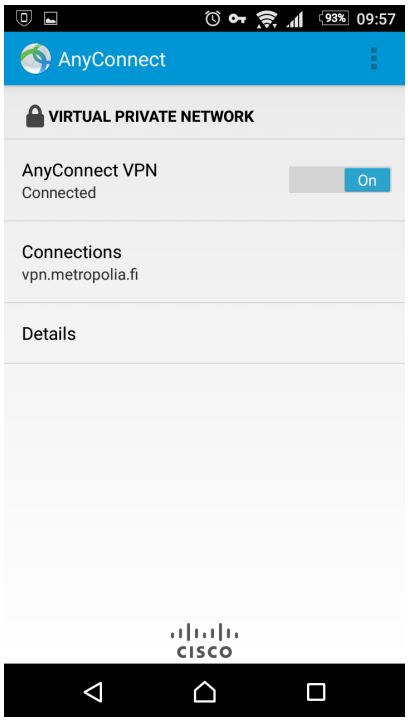
5. Lue tarkemmat asennusohjeet Windows-tietokoneita varten täältä: VPN-apuohjelman asennus ja käyttö omassa Windows-tietokoneessa.

VPN-apuohjelman asennus ja käyttö mobiililaitteissa

1. Hae AnyConnect-apuohjelma hakusanoilla "cisco secure client", "anyconnect" tai "cisco anyconnect" valmistajakohtaisesta sovelluskaupasta.



2. Asenna sovellus mobiililaitteeseen.
3. Lisää uusi VPN-yhteys kohdasta Connections > Add New Connection.
4. Kirjoita kohtaan Server Address osoite vpn.metropolia.fi
5. Valitse Done.
7. Käynnistä yhteys valitsemalla AnyConnect VPN.



8. Syötä Metropolian tunnus ja salasana.

9. Kirjaudu ulos valitsemalla ylhäältä oikealta Exit, kun katkaiset yhteyden.

Yhteyden ollessa suojattu Androidin yläpalkissa on lukon kuva ja iPhonen yläpalkissa on teksti VPN.

VPN-etäyhteyden käyttö Metropolian ylläpitämissä Windows-tietokoneissa

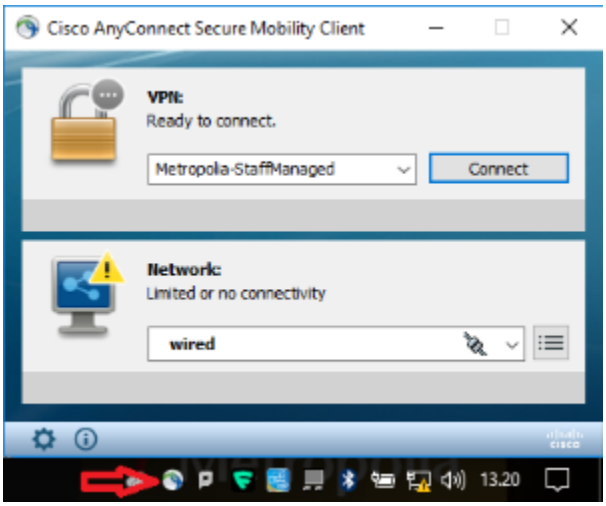
Jos kannettavasi on asennettu tai uudelleen asennettu syksyllä 2022 tai sen jälkeen, voit avata VPN-yhteyden ennen kirjautumista Windowsiin. Ks. VPN-yhteyden avaaminen ennen Windowsiin kirjautumista.

1. Klikkaa tietokoneesi ruudun oikeasta alanurkasta löytyvää Cisco AnyConnect -kuvaketta.

2. Valitse "Ready to connect" -tekstin alapuolelta alasvetovalikosta "Metropolia-StaffManaged" tai opiskelijakoneissa "Metropolia-StudentManaged".

3. Klikkaa Cisco AnyConnect Secure Mobility Client -ikkunan VPN-osiosta löytyvää Connect-painiketta.

4. Kirjaudu palveluun omalla Metropolian käyttäjätunnuksellasi.



VPN-apuohjelman asennus ja käyttö Apple macOS-tietokoneissa

macOS 11 Big Sur ja uudemmat macOS-versiot

Jos koneessasi on macOS 11 Big Sur tai uudempi käyttöjärjestelmä niin katso allaolevan linkin ohje AnyConnectin asennuksen jälkeisiin alkutoimiin.
Cisco AnyConnect, macOS 11 Big Sur +

Ilman näitä toimenpiteitä AnyConnect ei toimi!

Tietohallinnon ylläpitämiin Apple macOS-tietokoneisiin Cisco AnyConnect-ohjelma asentuu automaattisesti Managed Software Center-ohjelman päivitysten kautta.

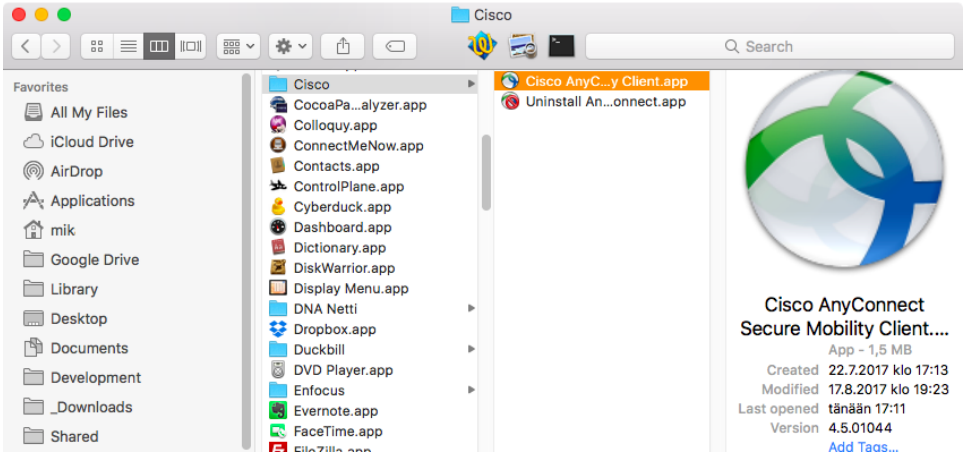
Jos kone on omasi niin voit ladata ja asentaa VPN-ohjelman seuraavalla tavalla:

1. Kirjaudu osoitteeseen https://vpn.metropolia.fi
2. Valitse vasemmalta AnyConnect.
3. Valitse Start AnyConnect.

Ohjelma asentuu paikkaan: **/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app**.

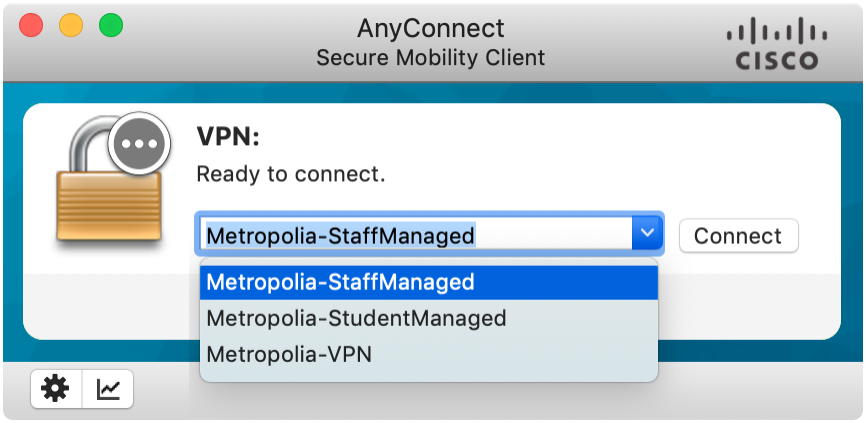
VPN-etäyhteys käynnistetään seuraavasti:

1. Avaa **/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app**.



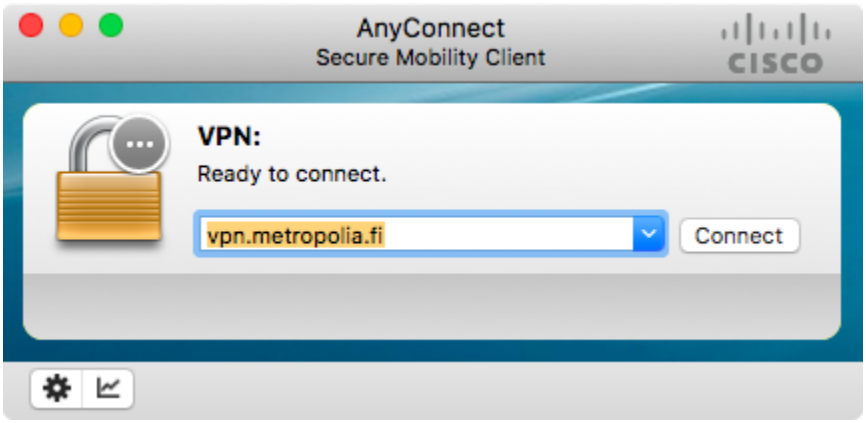
2. VPN-yhteysprofiilin valinta

a) Mac-kone joka on Metropolian ylläpitämä
Valitse "Ready to connect" -tekstin alapuolelta alasvetovalikosta "Metropolia-StaffManaged".
Opiskelijoiden käyttämissä ylläpidetyissä Mac-koneissa valitaan "Metropolia-StudentManaged".



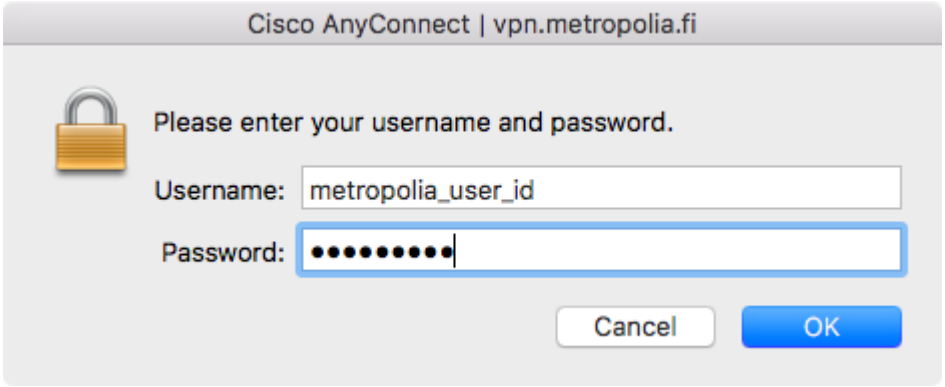
Osoitteen valinnan jälkeen paina "**Connect**".

b) Mac-kone joka ei ole Metropolian ylläpitämä tai osoitekentässä ei lue valmiiksi mitään, kirjoita kenttään osoitteeksi: **vpn.metropolia.fi**.

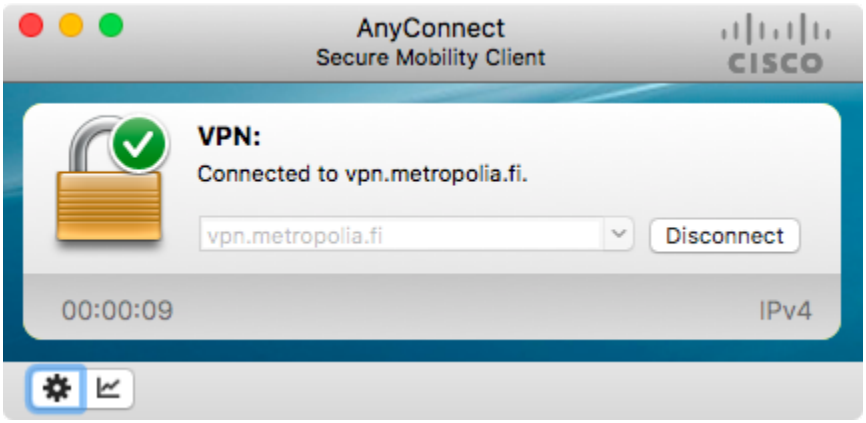


Osoitteen valinnan jälkeen paina "**Connect**".

3. Anna Metropolia-tunnuksesi ja sen salasana. Sitten paina "**OK**".



4. Kun yhteys on muodostunut niin yhteysikkuna näyttää tältä:



AnyConnect VPN-yhteyden tilan voi myös todeta ylävalikon pienestä AnyConnect-kuvakkeesta.

Kun yhteys on kunnossa niin kuvakkeessa on pieni suljetun lukon kuva:

VPN-yhteyden sulkeminen tapahtuu lopettamalla AnyConnect-ohjelma.

VPN-yhteydessä on myös aikaraja jolloin käyttämätön VPN-yhteys suljetaan.

Yhteys katkeaa automaattisesti myös silloin kun tietokone sammutetaan tai laitetaan nukkumaan.

VPN-etäyhteydellä saatavat palvelut

VPN-yhteydellä saatavat palvelut riippuvat sekä käyttäjän roolista että käytetystä päätelaitteesta. Tietoturvasyistä etäyhteydellä saatavaa pääsyä sisäisiin resursseihin rajoitetaan.

VPN-etäyhteyttä käytettäessä käyttäjän tietoliikenne on lähtöisin Metropoliasta, jolloin VPN-yhteydellä voi käyttää etänä sellaisia internet-palveluita, jotka ovat rajattu Metropoliaan käyttäjän IP-osoitteen perusteella, tai joihin tarvitaan suomalainen lähdeosoite.

VPN-etäyhteydellä saatavia palveluita voidaan rajoittaa tilapäisesti tai pysyvästi tietoturvatilanteen niin vaatiessa.

Metropolian ylläpitämät laitteet

Metropolian ylläpitämillä laitteilla on käytettävissä käyttäjän roolin mukaisesti pääsääntöisesti samat palvelut kuin henkilökunnan työasemilla ja digitilojen työasemilla. Tietoturvasyistä levypalvelut ja monet muut sisäiset resurssit ovat käytettävissä etänä vain Metropolian omistamilla laitteilla, joiden tietoturvasta vastaa Metropolian tietohallinto.

Käyttäjien omat laitteet

Käyttäjien omien laitteiden teknisen tietoturvan tasoa ei kontrolloida millään tavalla, mikä mahdollistaa VPN-palveluiden tarjoamisen kaikille käyttäjille ja laitteille, mutta johtaa rajoitettuun pääsyyn. Pääsääntöisesti omilta laitteilta on pääsy sekä henkilökunnan että opiskelijoiden selainkäyttöisiin sisäisiin järjestelmiin. Tietokantayhteyksiä, lisenssejä ja muita sisäisiä resursseja vaativien palveluiden käyttö omilla laitteilla harkitaan tapauskohtaisesti perustuen tietoturvariskiin, joka heikosti ylläpidetystä laitteesta mahdollisesti aiheutuu.

Opetuksen osalta omilla laitteilta on pääsy soveltuvin osin mm. educloudin virtuaalipalvelimiin, projektipalvelimiin ja laboratorioympäristöihin. Opetuksessa käytettävien järjestelmien osalta etäkäyttöä voi tietoturvan lisäksi rajoittaa taustajärjestelmien ja sovellusten lisenssiehdot.

Muut etäkäyttöpalvelut

Muita tapoja käyttää etänä Metropolian IT-paveluita ovat mm.

- Securedesktop-etätyöpöytä henkilökunnalle, Securedesktop-etätyöpalvelu
- SSH-tunnelointi, SSH-tunnelointi
- Verkkolevyjen selainliittymä, https://webdisk.metropolia.fi
- Kirjaston tietokannat, http://ezproxy.metropolia.fi ja ohjeet

VPN-rajoitukset

Käytä VPN-yhteyttä vain silloin kun oikeasti tarvitset sitä ja harkiten riittävän kapasiteetin varmistamiseksi!

Älä käytä verkko-opetusalustojen, videoneuvottelupalveluiden tai videoiden katselun yhteydessä VPN-yhteyttä.

VPN-etäyhteydellä saatavia palveluita voidaan rajoittaa tilapäisesti tai pysyvästi tietoturvatilanteen tai kriittisten palveluiden saavutettavuuden niin vaatiessa.
Metropolian VPN-yhteyttä ei ole mitoitettu kriisitilanteita varten.

OMA, Moodle, Zoom, Teams tai Skype for Business eivät tarvitse VPN-yhteyttä toimiakseen.

Huom. Ulkomaanmatkalla on muistettava, että työskennellessä kaikkia verkkoyhteyksiä on käytettävä aina VPN-yhteyden kanssa, mukaan lukien lankaverkot ja salasanalla suojatut verkkoyhteydet. VPN-yhteys suojaa datan kryptauksella, jolloin ulkopuolinen ei pysty lukemaan verkkoliikenteessä liikkuvaa dataa. Varmista ennen matkaasi VPN-yhteyden toimivuus.